DOE/IG-0459

AUDIT REPORT

UNCLASSIFIED COMPUTER NETWORK SECURITY AT SELECTED FIELD SITES

FEBRUARY 2000

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF AUDIT SERVICES

February 15, 2000

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (Signed)
Inspector General

SUBJECT: INFORMATION: Report on "Unclassified Computer Network Security at Selected Field Sites"

BACKGROUND

Improving security for unclassified information systems is one of the top issues facing government organizations today. This issue developed as Federal agencies migrated from a closed architecture, limited-access, mainframe environment to a web-based, client/server architecture, where literally the world may access government systems. The U.S. General Accounting Office (GAO) confirmed this reality in a series of reports to the Congress culminating in the designation of information system security as a “new Government-wide high-risk area.”

As recognized by GAO and other Federal standard setting bodies, organizations should adopt a risk-based approach to improving unclassified computer network security. The cost and benefit of controls, as well as the severity, probability, and extent of potential harm, should be considered when designing security improvements. The cost of improvements should not exceed expected benefits, and should be appropriate and proportionate to the value and degree of reliance on the information protected.

Complex-wide, the Department of Energy (Department) expends a significant portion of its budget to maintain a series of interconnected unclassified networks and information technology systems. In both Fiscal Years (FY) 1998 and 1999, the Department spent over $1.5 billion each year (almost 10 percent of its total budget) on information technology resources, including financial management systems. Organizations within the Department have numerous interconnected network systems that are utilized to meet day-to-day mission requirements including financial, security, and/or research activities. Connection of these networks to systems, such as the Energy and Sciences Network and the Department of Energy Business Network, permit the exchange of data between virtually all of the Department’s sites and components. The objective of the audit was to determine whether the internal controls employed for certain Department and contractor operated information systems were protecting such systems from malicious attack by internal and external parties.

RESULTS OF AUDIT

All six Departmental sites audited had significant internal or external weaknesses that increased the risk that their unclassified computer networks could be damaged by malicious attack. Specifically, each site had network vulnerabilities involving:

- Poor password management – Weak, non-existent or default passwords for regular users, network administrators, and security personnel were present on virtually all of the networks reviewed.

- Unnecessary access to certain powerful computer services and weak configuration management - Users had access to a number of services not specifically required for performance of their duties. File transfer and remote access services had not been configured to reduce vulnerabilities or were not required for network operation.

- Outdated software with known security vulnerabilities and firewall configuration problems – Operating system and application software with known exploitable weaknesses had not been replaced with updated versions. Firewall configuration problems at three sites inappropriately permitted certain traffic in and out of the networks.

Even though the Department became aware of a number of network security problems in recent years, it did not issue specific network security requirements until recently. In the absence of specific Departmental requirements, sites had not implemented a comprehensive network security program designed to test for password or configuration management issues or other internal and external vulnerabilities. The problems observed increased the risk that the Department's unclassified computing and network resources could be penetrated by unauthorized or malicious knowledgeable insiders and external "hackers." Unauthorized users could obtain information that could permit them to damage or disable Departmental networks by the alteration, deletion, or theft of sensitive data. Systems were also susceptible to widespread damage that could be caused by the installation of malicious software.

MANAGEMENT REACTION

The Chief Information Officer (CIO) agreed, in principle, with the recommendations in this report. Management acknowledged that sites have taken action to eliminate actual vulnerabilities identified during the audit, utilizing a risk-based approach. The CIO stated that correction of vulnerabilities, in general, is a goal and that management is working to consistently and adequately implement Departmental Notice 205.1, "Unclassified Cyber Security Program." However, management indicated that there was some concern that the high-risk vulnerabilities identified during audit testing were, in reality, false positives.

With regard to our recommendation on performance measures, the CIO indicated that a set of metrics is being developed to measure the effectiveness of the Cyber Security Program (CSP) across the Department. From these metrics, a baseline will be created and implemented to demonstrate improvement in the Department's CSP.

Attachment

cc: Deputy Secretary
Under Secretary

UNCLASSIFIED COMPUTER NETWORK SECURITY AT SELECTED FIELD SITES

TABLE OF CONTENTS

Overview

Unclassified Computer Network Security at Selected Field Sites

Appendices

OVERVIEW

INTRODUCTION AND OBJECTIVE

Improving security for unclassified information systems is one of the top issues facing government organizations today. This issue developed as Federal agencies migrated from a closed architecture, limited-access, mainframe environment to a web-based, client/server architecture, where literally the world may access government systems. The U.S. General Accounting Office (GAO) confirmed this reality in a series of reports to the Congress culminating in the designation of information system security as a "new Government-wide high-risk area."

As recognized by GAO and other Federal standard setting bodies, organizations should adopt a risk-based approach to improving unclassified computer network security. The cost and benefit of controls, as well as the severity, probability, and extent of potential harm, should be considered when designing security improvements. The cost of improvements should not exceed expected benefits, and should be appropriate and proportionate to the value and degree of reliance on the information protected.

Complex-wide, the Department of Energy (Department) expends a significant portion of its budget to maintain a series of interconnected unclassified networks and information technology systems. In both Fiscal Years (FY) 1998 and 1999, the Department spent over $1.5 billion each year (almost 10 percent of its total budget) on information technology resources, including financial management systems. Organizations within the Department have numerous interconnected network systems that are utilized to meet day-to-day mission requirements including financial, security, and/or research activities. Connection of these networks to systems, such as the Energy and Sciences Network and the Department of Energy Business Network, permit the exchange of data between virtually all of the Department's sites and components.

The increasing reliance of Federal Government agencies on interconnected systems and electronic data has increased the risk of fraud, inappropriate disclosure of sensitive data, and disruption of critical operations and services. Various audit reports issued by Federal agencies from March 1996 through August 1998 identified significant information security weaknesses. Poor control over access to sensitive data and systems was a widely reported weakness. Access weaknesses provide opportunities for an individual or group to disrupt agency operations by inappropriately modifying or destroying sensitive data or programs, obtaining or disclosing confidential information, or performing other malicious or unauthorized operations.

Network vulnerability and penetration testing assesses whether an organization's information technology security countermeasures are effective in preventing compromises. Sometimes referred to as "ethical" or "white-hat" hacking, penetration testing is the use of "hacker tools" and techniques and other security testing tools, within a methodical framework, to provide a "real-life" test of systems for vulnerabilities.
Penetration testing can counter threats by identifying technical vulnerabilities in networks and specific systems as well as weaknesses in security policies, standards, and procedures.

The objective of the audit was to determine whether the internal controls employed for certain Department and contractor operated information systems were protecting such systems from malicious attack by internal and external parties. The audit was performed as part of the Office of Inspector General's (OIG) continuing effort with respect to the Department's compliance with the Government Performance and Results Act (GPRA) of 1993.

CONCLUSIONS AND OBSERVATIONS

All six Departmental sites audited had significant internal or external weaknesses that increased the risk that their unclassified computer networks could be damaged by malicious attack. Each site had internal network vulnerabilities involving poor password management, unnecessary access to certain powerful computer services, weak configuration management, and/or outdated software with known security problems. Externally, we observed problems with firewall configuration and virtually all of the same problems observed during internal network testing, although to a lesser extent. Even though the Department became aware of a number of network security problems in recent years, it did not issue specific network security requirements until recently. In the absence of specific Departmental requirements, sites had not implemented a comprehensive network security program designed to test for password or configuration management issues or other internal and external vulnerabilities. The problems observed increased the risk that the Department's unclassified computing and network resources could be penetrated by unauthorized or malicious knowledgeable insiders and external "hackers." Unauthorized users could obtain information that could permit them to damage or disable Departmental networks by the alteration, deletion, or theft of sensitive data. Systems were also susceptible to widespread damage that could be caused by the installation of malicious software.

The Chief Information Officer (CIO) concurred, in principle, with the recommendations made in this report.

Management should also consider the issues discussed in this report when preparing the yearend assurance memorandum on internal controls.

(Signed)
Office of Inspector General

Information Resources are at Risk

Significant internal or external weaknesses existed on selected systems and devices attached to the computer networks at the six Department sites audited.[1] These weaknesses in automated security controls increased the risk that the site computer networks could be damaged by malicious attack. Each site had internal network vulnerabilities involving poor password management, unnecessary access to certain powerful computer services, weak configuration management, and/or outdated software with known security problems. Externally, we observed problems with firewall configuration and virtually all of the same problems noted during internal network testing, although to a lesser extent.

Password Management

Password management problems could adversely affect network operation and security at each of the locations audited. To varying degrees, each site had problems with regular user passwords, those used by network administrators and security personnel, or passwords used to access certain computer services such as file transfer routines. Accounts or services without passwords, or those with default passwords, were present on eight of the nine computer networks audited at the six sites visited. Passwords that were identical to the user identification for certain workstations and servers were also observed. Weaknesses, such as those observed, could permit unfettered access to virtually all system resources and increase the risk of network compromise or shutdown.

Services and Configuration Management

All sites audited had security vulnerabilities associated with unnecessary services and configuration management. Certain services involving file sharing and transfer were active even though they were not required by the user. Other file transfer and remote access services had not been properly configured or were not specifically required for system operation. Unnecessary services/configuration management issues can arise when changes are made to network structure, or when a system or device is first attached to a network. Each device or system comes initially configured with certain services that may not be needed and certain default parameters that may not be secure. Therefore, as a general rule, computing devices must be tailored to fit the network in terms of not only functionality, but also security to mitigate vulnerabilities.

[1] For security reasons, specific information as to location and type of vulnerability has been omitted from the report. Details regarding our finding were provided to management at each of the sites audited.

Software Security Vulnerabilities and Firewalls

Outdated versions of software with known security vulnerabilities and firewall installation or configuration problems were also present on the networks at the sites visited. We found outdated versions of operating system software on devices that route and filter network traffic. Application software with known security vulnerabilities was also observed. Operating system and application software can contain inherent or hacker exploitable vulnerabilities, which, if not corrected, could allow unauthorized access to systems and devices. Despite Departmental recognition that the effective use of firewalls should be considered the starting point for enhancing unclassified network security, one site did not have a firewall and another had not installed a previously procured firewall. At least three networks at the sites reviewed had firewall configuration problems that inappropriately allowed certain traffic in and out of the networks.

Federal and Departmental Directives Require Information Resource Security

Office of Management and Budget Circular A-130 requires Federal agencies to establish a level of security for all information systems that is commensurate with the risk and magnitude of the harm that would result from the loss, misuse or unauthorized access to, or modification of the information contained in these information systems. Other Federal and Departmental directives require that procedures be developed and implemented to prevent misuse and abuse of unclassified computing or information technology resources.

Presidential Decision Directive (PDD) 63, issued on May 22, 1998, recognized that additional attention to cyber security and protection of the Nation's critical infrastructure was required. The directive recognized that a single network compromise can affect a multitude of systems. It also required Federal agencies to work to reduce exposure to security threats and significantly increase security for government systems by the year 2000.

Despite Awareness of Network Security Problems, the Department was Slow to Act

Even though awareness of network security problems increased substantially in the last several years, the Department did not issue specific network security requirements until recently. Awareness increased during 1997 and 1998, as the Office of Oversight issued a series of reports demonstrating that networks throughout the Department were vulnerable to attack. Departmental security officials also reported that penetrations and "hacking" incidents escalated and less attention was paid to network security during that same period. In addition, the Department identified unclassified computer security as a "Departmental Challenge" in the FY 1998 Accountability Report. The Accountability Report pointed out that the system of controls was not operating effectively and did not provide reasonable assurance that assets or resources were safeguarded against fraud, waste, abuse, and mismanagement. Despite the increase in awareness, the Department did not issue specific network security requirements until July 1999. In the absence of specific Departmental guidance, sites and programs developed and implemented network security programs with varying levels of rigor.

While each of the sites audited had developed and implemented certain policies, procedures and physical controls to protect computer systems, comprehensive network security programs were not in place. Network security programs were not consistent from site to site, and some programs omitted tests for password management and control, configuration management, or other internal and external vulnerability tests. Network security scanning or testing was either informal and/or infrequent, or the testing tools utilized were insufficient for performing comprehensive testing of the network environment. Baselines and standard parameter settings for conducting tests of network security had largely not been formally established.

In addition, we found that specific performance measures and objectives for network security had not been established. Even though the Department had designated unclassified computer security as a "Departmental Challenge" during the FY 1998 Federal Managers' Financial Integrity Act process, specific goals or measures had not been established as required by GPRA. In the absence of such goals, responsible site personnel were not giving sufficient priority to addressing computer network security concerns. For instance, site personnel were generally not required to test for network vulnerabilities and limited their security functions to updating computer security plans and reporting on computer application recertifications.

Vulnerabilities Could Impact Unclassified Information Security for the Entire Department

Exploitation of the network security weaknesses described in this report could lead to a potentially serious and costly disruption of the Department's operations. Unauthorized or malicious individuals ("hackers") could modify or destroy sensitive data or programs, steal or improperly disclose confidential information, or perform other malicious or unauthorized operations. A knowledgeable insider or an external "hacker," using tools readily available on the Internet, could exploit network interconnectivity by using one vulnerable system to gain access to similar systems or devices on networks throughout the complex. The potential for harm is substantial in that many of the Department's interconnected systems are utilized to meet day-to-day mission requirements such as financial, security, and/or research activities. Once a network is penetrated, attackers could potentially do harm to systems at other Departmental sites.

Near the end of our audit field work, the Department launched a new initiative designed to improve network security across the complex. On July 26, 1999, the Department published Departmental Notice 205.1, “Unclassified Cyber Security Program” (Notice). The purpose of the Notice was to protect the Department’s distributed network environment and require a contemporary and proactive approach to computer security. Concurrent with the issuance of this Notice, the Department embarked on a complex-wide program to provide additional training for network system administrators and security personnel, raise user awareness of security issues, and generally improve network security. The Notice specifically required each site and program element to improve network security by developing specific computer/network security plans, actions, policies, and procedures.

This new directive should greatly advance the Department’s network security position, mitigate the problems specified in this audit report, and generally enhance its ability to protect cyber related critical infrastructure. However, the specific vulnerabilities disclosed during the audit and separately conveyed to site managers need to be addressed. To aid in this effort, detailed action plans, with associated performance measures, need to be developed. As an interim solution, each of the sites visited has initiated action to correct specific vulnerabilities identified in this report.

Meaningful and measurable performance measures, with specific achievable goals, are essential to ensuring the success of the Department’s network security improvement initiative. Without specific performance standards or measures, the Department cannot ensure that the goal of PDD 63, to swiftly eliminate any significant vulnerability to cyber attacks on our computer networks, will be achieved. In addition, the Department cannot ensure that the PDD 63 requirement that any interruption or manipulation of computer networks be brief, infrequent, manageable, and minimally detrimental.

As the Department moves forward with network security improvements, it must ensure that the cost of improvements, in both monetary and non-monetary terms, does not exceed expected benefits. As emphasized by the new Notice, network security improvements (and associated performance measures) should be developed and implemented using a risk-based approach. Performance goals should incorporate the concept that protection should be appropriate and proportionate to the value and degree of reliance on systems. The cost and benefit of controls, as well as the severity, probability, and extent of potential harm, should be considered when designing meaningful performance measures.

RECOMMENDATIONS

The new Notice should enable the Department to better ensure that controls are in place to safeguard information and technology resources from unauthorized access. However, the CIO, in conjunction with Lead Program Secretarial Officers and Managers of various field activities, commensurate with a risk-based approach, needs to:

1. Resolve to fully implement the new Notice, and ensure that the security vulnerabilities disclosed during this audit are corrected; and

2. In accordance with GPRA, establish specific goals and performance measures for improving the level of unclassified computer security relating to network operations.

MANAGEMENT REACTION

The CIO agreed, in principle, with the recommendations in this report. Management acknowledged that sites have taken action to eliminate actual vulnerabilities identified during the audit, utilizing a risk-based approach. The CIO stated that correction of vulnerabilities, in general, is a goal and that management is working to consistently and adequately implement the new Notice. However, management indicated that there was some concern that the high-risk vulnerabilities identified during audit testing were, in reality, false positives.

With regard to our recommendation on performance measures, the CIO indicated that a set of metrics is being developed to measure the effectiveness of the Cyber Security Program (CSP) across the Department. From these metrics, a baseline will be created and implemented to demonstrate improvement in the Department's CSP.

AUDITOR COMMENTS

We consider the CIO's comments and site actions generally responsive to the issues addressed in this report. However, we do not agree that any significant portion of the high-risk vulnerabilities identified during audit testing were false positives. The vulnerabilities were discovered using tools that are commonly employed by information technology and security professionals, including GAO, the Department's Computer Incident Advisory Capability and the Office of Oversight. These tools are routinely used by the above organizations to survey network security at certain Department sites and are considered to be reliable.

Although we endeavored to do so, we may have been unable to definitively eliminate all false positives from the report because several of the sites audited elected not to provide detailed responses to our queries. At least one site indicated that it would not devote the time and effort necessary to review each of the reported vulnerabilities. Another site acknowledged that our audit disclosed a number of vulnerabilities and that they were working to correct them, but did not respond to our repeated requests to identify false positives.

Appendix 1

SCOPE

The audit work was performed between September 1998 and September 1999. We performed a vulnerability assessment of computing network operations with the focus being on segments containing financial applications. Specifically, we assessed the automated system security controls relating to network operations to determine the effectiveness of parameter settings and uncover weaknesses in access controls for safeguarding information resources from unauthorized internal and external sources. The audit did not include an overall review of general controls, in such areas as application software development and change controls, service continuity, or user authorizations. In addition, our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent the existing controls.

METHODOLOGY

To accomplish our objectives, we obtained and reviewed applicable directives pertaining to security of information and information technology resources, such as OMB Circular A-130, GPRA, PDD 63, Departmental Notice 205.1, Departmental Order 471.2A "Information Security Program," Departmental Order 1360.2B "Unclassified Computer Security Program," Federal Information Processing Standards Publication 191 "Guidelines for the Analysis of Local Area Network Security," and Executive Order 13011 "Federal Information Technology." We also reviewed reports by the OIG, the Office of Oversight, operations offices and various internal groups. Officials and staff were interviewed at the Department's Headquarters locations, operations offices, and contractor operated facilities.

We gained an understanding of controls surrounding network and computing operations, such as communication services and operating systems, through inquiry, observation, and document inspection, and noted the existence of controls.

We did not rely on computer processed data generated by the sites audited to satisfy our audit objectives. We did, however, use a number of computer-assisted audit tools to perform probes of various networks and devices. We validated the results of our scans by confirming the weaknesses disclosed with responsible site personnel.

The audit was conducted in accordance with generally accepted Governmental auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objectives.

Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed. Also, projection of any evaluation of the structure to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate. An exit conference was held with CIO representatives on January 20, 2000.

PRIOR OFFICE OF INSPECTOR GENERAL REPORTS

- *Audit of Departmental Integrated Standardized Core Accounting System (DISCAS) Operations at Selected Field Sites,* Office of Inspector General Report No. AP-FS-97-02, dated June, 1997. The report pointed out that some weaknesses existed in the general and application controls for DISCAS that could adversely affect the reliability of data processed through the system.

- *Audit of the ADP General Controls at Idaho National Engineering and Environmental Laboratory,* Office of Inspector General Report No. CR-FS-L-98-01, dated February 1998. The report stated that, although general controls had been established for ensuring that application controls could not be rendered ineffective by circumvention or modification, further enhancements were needed to ensure proper security over sensitive computer systems and data.

- *Audit of the ADP General Controls at Oak Ridge Complex,* Office of Inspector General Report No. CR-FS-L-98-02, dated February 1998. The report stated that, although general controls had been established for ensuring that application controls could not be rendered ineffective by circumvention or modification, further enhancements were needed to ensure proper security over computer systems and data.

- *Report on Matters Identified at the Oakland Operations Office During the Audit of the Department of Energy's Consolidated Fiscal Year 1998 Financial Statements,* Office of Inspector General Report No. WR-FS-99-04, dated May 1999. The report stated that, several networks and various network components were not adequately protected and were vulnerable to unauthorized access. The OIG concluded that strengthening was needed in computer network security.

- *Management Report on Audit of the Department of Energy's Consolidated Financial Statements for Fiscal Year 1998,* Office of Inspector General Report No. CR-FS-99-01, dated June 1999. The report pointed out that the network backbone and various network components were not adequately protected and were vulnerable to unauthorized access and malicious attack. The OIG concluded that, without strengthening computer network security, weaknesses could result in breaches in the security of data and programs.

- *Matters Identified at the Savannah River Operations Office During the Audit of the Department's Consolidated Fiscal Year 1998 Financial Statements,* Office of Inspector General Report No. ER-FS-99-03, dated May 1999. The report pointed out that, although policies, procedures and physical controls to protect computer programs and data files had been implemented, certain vulnerabilities existed on selected systems and devices. The OIG concluded that, without improvements in security controls, risk is increased for unauthorized access to the computer network.

IG Report No. :DOE/IG-0459

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in this report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name ______________________________ Date __________________________

Telephone __________________________ Organization ____________________

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following alternative address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.